Construction of rate (n — 1)/n non-binary LDPC convolutional codes via difference triangle sets

Alfarano, Gianira Nicoletta ; Lieb, Julia ; Rosenthal, Joachim

Abstract: This paper provides a construction of non-binary LDPC convolutional codes, which generalizes the work of Robinson and Bernstein. The sets of integers forming an (n - 1,w)- difference triangle set are used as supports of the columns of rate (n - 1)/n convolutional codes. If the field size is large enough, the Tanner graph associated to the sliding parity-check matrix of the code is free from 4 and 6-cycles not satisfying the full rank condition. This is important for improving the performance of a code and avoiding the presence of low-weight codewords and absorbing sets. The parameters of the convolutional code are shown to be determined by the parameters of the underlying difference triangle set. In particular, the free distance of the code is related to w and the degree of the code is linked to the "scope" of the difference triangle set. Hence, the problem of finding families of difference triangle set with minimum scope is equivalent to find convolutional codes with small degree.

DOI: https://doi.org/10.1109/isit44484.2020.9174510

Construction of Rate $(n-1)/n$ Non-Binary LDPC Convolutional Codes via Difference Triangle Sets

Gianira Nicoletta Alfarano
University of Zurich
Switzerland
gianiranicoletta.alfarano@math.uzh.ch

Julia Lieb
University of Zurich
Switzerland
julia.lieb@math.uzh.ch

Joachim Rosenthal
Fellow, IEEE
University of Zurich
Switzerland
rosenthal@math.uzh.ch

***Abstract*—This paper provides a construction of non-binary LDPC convolutional codes, which generalizes the work of Robinson and Bernstein. The sets of integers forming an $(n-1,w)$-difference triangle set are used as supports of the columns of rate $(n-1)/n$ convolutional codes. If the field size is large enough, the Tanner graph associated to the sliding parity-check matrix of the code is free from 4 and 6-cycles not satisfying the full rank condition. This is important for improving the performance of a code and avoiding the presence of low-weight codewords and absorbing sets. The parameters of the convolutional code are shown to be determined by the parameters of the underlying difference triangle set. In particular, the free distance of the code is related to w and the degree of the code is linked to the "scope" of the difference triangle set. Hence, the problem of finding families of difference triangle set with minimum scope is equivalent to find convolutional codes with small degree.**

I. Introduction

The aim of this paper is to construct a family of non-binary low-density parity-check (NB-LDPC) convolutional codes suitable for iterative deoding. The class of LDPC block codes was introduced by Gallager [8]. Their name is due to the fact that they have a parity-check matrix that is sparse. Similarly to LDPC block codes, one can construct LDPC convolutional codes as codes whose sliding parity-check matrices are sparse, which allows them to be decoded using iterative message-passing algorithms.

In the last few years, some attempts to construct binary LDPC convolutional codes were done. However, most of the constructions are for time-varying convolutional codes, see for instance [2], [14], [18].

In 1967, Robinson and Bernstein [15] used difference triangle sets for the first time to construct binary recurrent codes, which are defined as the kernel of a binary sliding parity-check matrix. At that time, the theory of convolutional codes was not developed yet and the polynomial notation was not diffused, but now, we may regard recurrent codes as a first version of convolutional codes. This was the first time that a combinatorial object was used to construct convolutional codes. Three years later, Tong in [16], used diffuse difference triangle sets to construct self-orthogonal diffuse convolutional codes, defined by Massey [12]. The aim of these authors was to construct codes suitable for iterative decoding and their result was a rudimental version of binary LDPC convolutional codes.

In this paper, we exploit the structure of difference triangle sets to construct non-binary LDPC convolutional codes whose parity check matrices are free from 4-cycles and 6-cycles not satisfying the so called full rank condition. Our construction may be regarded as a generalization over $\mathbb{F}_q$ of the construction of Robinson and Bernstein. We describe a close link between the properties of the difference triangle set and the parameters of the code. Moreover, we derive information on the column distances and on the free distance of the constructed codes, by exploiting the structure of the underlying difference triangle set.

The paper is structured as follows. In Section II, we first give some useful basics of the theory of convolutional codes and then we define difference triangle sets and their scope. In Section III, we define non-binary LDPC block codes and non-binary LDPC convolutional codes. In Section IV, we give a new construction of rate $(n-1)/n$ non-binary LDPC convolutional codes, starting from an $(n-1,w)$ difference triangle set. We show how the parameters of the code are related to the properties of the triangle set and we point out that several research works in combinatorics can be exploited to improve our construction. We derive some distance properties of the codes and the exact formula for computing their density. We conclude with further comments and future research directions in Section V.

II. Preliminaries

A. Convolutional Codes

Let q be a prime power, $\mathbb{F}_q$ be the finite field of order q and k,n be positive integers, with $k<n$. A rate-k/n convolutional code over $\mathbb{F}_q$ is a submodule $\mathcal{C}$ of $\mathbb{F}_q[z]^n$ of rank k, such that there exists a $k\times n$ polynomial generator matrix $G(z)\in\mathbb{F}_q[z]^{k\times n}$ which is *basic* and *reduced*, i.e., it has a right polynomial inverse and the sum of the row degrees of $G(z)$ attains the minimal possible value such that

$$\mathcal{C}:=\{u(z)G(z)\mid u(z)\in\mathbb{F}_q[z]^k\}\subseteq\mathbb{F}_q[z]^n.$$

The authors acknowledge the support of the Swiss National Science Foundation grant n. 188430. Julia Lieb acknowledges also the support of the German Research Foundation grant LI 3101/1-1.

If $G(z)$ is a reduced, basic generator matrix for $\mathcal{C}$, there exists a full row rank *parity-check* matrix $H(z) \in \mathbb{F}_q[z]^{(n-k)\times n}$ such that

$$\mathcal{C} := \{v(z) \in \mathbb{F}_q[z]^n \mid H(z)v(z)^\top = 0\}.$$

We define the *degree* δ of $\mathcal{C}$ as the highest degree of the $k \times k$ full size minors in $G(z)$. We denote a convolutional code of rate k/n and degree δ by $(n, k, \delta)_q$. For a polynomial vector $v(z) = \sum_{i=0}^{r} v_i z^i \in \mathcal{C}$, we define the *weight* of $v(z)$ as $\mathrm{wt}(v(z)) := \sum_{i=0}^{r} \mathrm{wt}(v_i) \in \mathbb{N}_0$, where $\mathrm{wt}(v_i)$ denotes the Hamming weight of $v_i \in \mathbb{F}_q^n$. The *free distance* of a convolutional code $\mathcal{C}$, $\mathrm{d_{free}}(\mathcal{C})$, is defined as the minimum of the nonzero weights of the codewords in $\mathcal{C}$. The parameters δ and $\mathrm{d_{free}}$ are needed to determine respectively the decoding complexity and the error correction capability of a convolutional code with respect to some decoding algorithm. For this reason, for any given rate k/n and field size q, the aim is to construct convolutional codes with "small" degree δ and "large" free distance $\mathrm{d_{free}}$.

Remark 1. There is a natural isomorphism between $\mathbb{F}_q[z]^n$ and $\mathbb{F}_q^n[z]$ that allows to consider a generator and a parity-check matrix of a convolutional code as polynomials whose coefficients are matrices. In particular, we will consider $H(z) \in \mathbb{F}_q^{(n-k)\times n}[z]$, such that $H(z) = H_0 + H_1 z + \dots H_\mu z^\mu$, with $\mu > 0$. With this notation, we can expand the kernel representation $H(z)v(z)^\top$ in the following way:

$$Hv^\top = \begin{bmatrix} H_0 & & & & & \\ \vdots & \ddots & & & & \\ H_\mu & \cdots & H_0 & & & \\ & \ddots & & \ddots & & \\ & & H_\mu & \cdots & H_0 & \\ & & & \ddots & \vdots & \\ & & & & H_\mu & \end{bmatrix} \begin{bmatrix} v_0 \\ v_1 \\ \vdots \\ v_r \end{bmatrix} = 0 \qquad (1)$$

We will refer to the representation of the parity-check matrix of $\mathcal{C}$ in equation (1) as *sliding parity-check matrix*.

For any $j \in \mathbb{N}_0$ we define the *j-th column distance of $\mathcal{C}$* as

$$\begin{aligned} d_j^c(\mathcal{C}) &:= \min_{v_0 \neq 0} \left\{ \mathrm{wt}(v_0 + v_1 z + \dots + v_j z^j) \mid v(z) \in \mathcal{C} \right\} \\ &= \min_{v_0 \neq 0} \left\{ \mathrm{wt}(v_0 + \dots + v_j z^j) \mid H_j^c [v_0 \cdots v_j]^\top = 0 \right\} \end{aligned}$$

with $H_j^c := \begin{bmatrix} H_0 & & & \\ H_1 & H_0 & & \\ \vdots & \vdots & \ddots & \\ H_j & H_{j-1} & \cdots & H_0 \end{bmatrix}$.

We recall the following result.

Theorem 2. *[9, Proposition 2.2] Let $d \in \mathbb{N}$. Then the following properties are equivalent.*

1) *$d_j^c = d$.*
2) *None of the first n columns of H_j^c is contained in the span of any other $d-2$ columns and one of the first n columns of H_j^c is in the span of some other $d-1$ columns of that matrix.*

B. Difference Triangle Sets

A difference triangle set is a collection of sets of integers such that any integer can be written in at most one way as difference of two elements in the same set. Difference triangle sets find application in combinatorics, radio systems, optical orthogonal codes and other areas of mathematics [3], [4], [10]. We refer to [5] for a more detailed treatment. More formally, we define difference triangle sets in the following way.

Definition 3. An (N, M)*-difference triangle set* (DTS) is a set $\mathcal{T} := \{T_1, T_2, \dots, T_N\}$, where for any $1 \leq i \leq N$, $T_i := \{a_{i,j} \mid 1 \leq j \leq M\}$ is a set of nonnegative integers such that $a_{i,1} < a_{i,2} < \dots < a_{i,M}$ and all the differences $a_{i,j} - a_{i,k}$, with $1 \leq i \leq N$ and $1 \leq k < j \leq M$ are distinct. When $N = 1$, we will refer to a $(1, M)$-DTS simply as DTS.

An important parameter characterizing an (N, M)-DTS $\mathcal{T}$ is the *scope* $m(\mathcal{T})$, that is defined as

$$m(\mathcal{T}) := \max\{a_{i,M} \mid 1 \leq i \leq N\}.$$

Observe that, a very well-studied problem in combinatorics is finding families of (N, M)-DTSs with minimum scope. In this work, we will use the sets in a DTS as supports of the columns in the sliding parity-check matrix of a convolutional code. We will relate the scope of the DTS with the degree of the code. Since we want to minimize the degree of the code, it is evident that the mentioned combinatorial problem plays a crucial role also here.

III. Low-Density Parity-Check Codes

A. Non-Binary LDPC Codes

In this section we briefly introduce LDPC block codes and we focus in particular on their non-binary version. We extend then the notion to LDPC convolutional codes.

LDPC codes are known for their performances near the Shannon-limit over the additive white Gaussian noise channel [11]. Their non-binary (NB-LDPC) version was first investigated by Davey and Mackay in 1998 in [6]. In [7], it was observed that NB-LDPC codes defined over a finite field with q elements can have better performances than the binary ones. A NB-LDPC code is defined as the kernel of an $N \times M$ sparse (at least 1/2 of the entries are zeros) matrix H with entries in $\mathbb{F}_q$. We can associate to H a bipartite graph $\mathcal{G} = (V, E)$, called *Tanner graph*, where $V = V_s \cup V_c$ is the set of vertices. In particular, $V_s = \{v_1, \dots, v_N\}$ is the set of *variable nodes* and $V_c = \{c_1, \dots, c_M\}$ is the set of *check nodes*. $E \subseteq V_s \times V_c$ is the set of edges, with $e_{n,m} = (v_n, c_m) \in E$ if and only if $h_{n,m} \neq 0$. The edge $e_{n,m}$ connecting a check node and a variable node is labelled by $h_{n,m}$, that is the corresponding *permutation node*. For an even integer ℓ, we call a simple closed path consisting of $\ell/2$ check nodes and $\ell/2$ variable nodes in $\mathcal{G}$ an *ℓ-cycle*. The length of the shortest cycle is called the *girth* of $\mathcal{G}$ or girth of H. It is proved that having higher girth decreases the decoding failure of the bit flipping algorithm. Moreover, in [13] the authors showed that short cycles in a NB-LDPC code may be harmful if they do not

satisfy the so called full rank condition (FRC). This is because if the FRC is not satisfied, the short cycles produce low-weight codewords or they form absorbing sets, [1].

In [13] and in [1] it is shown that an ℓ-cycle in a NB-LDPC code with parity check matrix H can be represented by an $\frac{\ell}{2} \times \frac{\ell}{2}$ submatrix of H of the form

$$A = \begin{bmatrix} a_1 & a_2 & 0 & \cdots & \cdots & 0 \\ 0 & a_3 & a_4 & \cdots & \cdots & \vdots \\ \vdots & & \ddots & & & \vdots \\ \vdots & & & \ddots & & \vdots \\ 0 & & & & a_{\ell-3} & a_{\ell-2} \\ a_\ell & 0 & \cdots & \cdots & 0 & a_{\ell-1} \end{bmatrix}, \qquad (2)$$

where $a_i \in \mathbb{F}_q^*$. The cycle does not satisfy the FRC if $\det(A) = 0$. In this case, the cycle gives an absorbing set. Hence, it is a common problem to construct NB-LDPC codes in which the shortest cycles satisfy the FRC.

The convolutional counterpart of NB-LDPC block codes is given by convolutional codes defined over a finite field $\mathbb{F}_q$ whose sliding parity-check matrix is sparse.

IV. Construction of Rate $(n-1)/n$ NB-LDPC convolutional Codes

In this section we will provide a construction of NB-LDPC convolutional codes over $\mathbb{F}_q$, with the aid of difference triangle sets. In a certain sense, this could be regarded as an extension over $\mathbb{F}_q$ of the construction given by Robinson and Bernstein.

Let $\mathbb{F}_q$ be the finite field of order $q = p^N$, where p is a prime number.

We are going to construct a sliding parity-check matrix as in equation (1). Observe that the decoding of a convolutional code $\mathcal{C}$ is done sequentially by blocks of length n, hence, the error-correcting properties of the code are determined by the decoding of the first block (see also [17]). In particular, it is sufficient to analyze the portion of the sliding parity-check matrix H which affects the decoding of the first block, namely

$$\mathcal{H} := H_\mu^c = \begin{bmatrix} H_0 & & & \\ H_1 & H_0 & & \\ \vdots & \vdots & \ddots & \\ H_\mu & H_{\mu-1} & \cdots & H_0 \end{bmatrix}. \qquad (3)$$

First of all, observe that since H_0 is full rank, one can perform Gaussian elimination on the block $\begin{bmatrix} H_0^\top & H_1^\top & \cdots & H_\mu^\top \end{bmatrix}^\top$, which results in the following block matrix:

$$\bar{H} = \begin{bmatrix} A_0 & | & I_{n-k} \\ A_1 & | & 0 \\ \vdots & & \vdots \\ A_\mu & | & 0 \end{bmatrix}, \qquad (4)$$

where $A_i \in \mathbb{F}_q^{(n-k)\times k}$ for $i = 1, \ldots, \mu$. With an abuse of notation, we will still write H_0 for indicating $[A_0 | I_{n-k}]$, and H_i for the matrices $[A_i | 0]$.

Note that it is important to construct the sliding parity-check matrix H of a NB-LDPC convolutional code such that the Tanner graph $\mathcal{G}$ associated to H does not contain short cycles not satisfying the FRC. It is easy to see that H satisfies this property if and only if $\mathcal{H}$ does. By the discussion of the previous section, this is equivalent to construct $\mathcal{H}$, such that all the 2×2 and 3×3 minors that are non-trivially zero, are non-zero.

In the following we focus on the construction of rate $(n-1)/n$ NB-LDPC convolutional codes. In particular, we will construct the matrices $A_i \in \mathbb{F}_q^{1\times(n-1)}$, such that the resulting matrix $\mathcal{H}$ does not contain 4-cycles and 6-cycles, not satisfying the FRC.

A. Construction

Let n, w be positive integers. Consider an $(n-1, w)$-DTS $\mathcal{T} := \{T_1, \ldots, T_{n-1}\}$. Each T_k will give the positions of the non-zero elements of the first $n-1$ columns of the matrix $\bar{H}$ of equation (4); the last column will be simply given by the vector $[1, 0, \ldots, 0]^\top$.

Definition 4. With the notation above, define the matrix $\bar{H}^{\mathcal{T}} \in \mathbb{F}_q^{m(\mathcal{T})\times n}$, in which the k-th column has weight w and support $T_k := \{a_{k,1}, \ldots, a_{k,w}\}$. Formally, let α be a primitive element for $\mathbb{F}_q$, so that any non-zero element of $\mathbb{F}_q$ can be written as power of α. For any $1 \le i \le m(\mathcal{T})$, $1 \le k \le n-1$,

$$\bar{H}_{i,k}^{\mathcal{T}} = \begin{cases} \alpha^{ik} & \text{if } i \in T_k \\ 0 & \text{otherwise} \end{cases}.$$

The last column of $\bar{H}^{\mathcal{T}}$ is given by $[1, 0, \cdots, 0]^\top$. Derive the matrix $\mathcal{H}^{\mathcal{T}}$ by "shifting" the columns of $\bar{H}^{\mathcal{T}}$ and then a sliding matrix $H^{\mathcal{T}}$ of the form of equation (1). Finally, define $\mathcal{C}^{\mathcal{T}} := \ker(\mathcal{H}^{\mathcal{T}})$ over $\mathbb{F}_q$. Note that here $\mu = m(\mathcal{T}) - 1$.

Example 5. Let $\mathbb{F}_q := \{0, 1, \alpha, \ldots, \alpha^{q-2}\}$ and $\mathcal{T}$ be a $(2, 3)$-DTS, such that $T_1 := \{1, 2, 6\}$ and $T_2 := \{1, 2, 4\}$. Then, with the notation above,

$$\bar{H}^{\mathcal{T}} = \begin{bmatrix} \alpha & \alpha^2 & 1 \\ \alpha^2 & \alpha^4 & 0 \\ 0 & 0 & 0 \\ 0 & \alpha^8 & 0 \\ 0 & 0 & 0 \\ \alpha^6 & 0 & 0 \end{bmatrix},$$

which leads to the sliding matrix in Figure 1.

Example 6. Let $\mathbb{F}_q := \{0, 1, \alpha, \ldots, \alpha^{q-2}\}$ and $\mathcal{T}$ be a $(2, 3)$-DTS, such that $T_1 := \{1, 2, 6\}$ and $T_2 := \{2, 3, 5\}$. Then, with the notation above,

$$\bar{H}^{\mathcal{T}} = \begin{bmatrix} \alpha & 0 & 1 \\ \alpha^2 & \alpha^4 & 0 \\ 0 & \alpha^6 & 0 \\ 0 & 0 & 0 \\ 0 & \alpha^{10} & 0 \\ \alpha^6 & 0 & 0 \end{bmatrix},$$

which leads to the sliding matrix in Figure 2.

Proposition 7. *Let $\mathcal{T}$ be an $(n-1,w)$-DTS with scope $m(\mathcal{T})$. Then, the code $\mathcal{C}^{\mathcal{T}}$ given as in Definition 4 is an $(n, n-1, m(\mathcal{T})-1)_q$ convolutional code.*

Remark 8. As already mentioned, an interesting problem in combinatorics is to find families of difference triangle sets having minimum scope [3], [5], [10]. This is a difficult task in general. For our application, it is desirable to have a difference triangle set $\mathcal{T}$ whose scope is as small as possible so that the degree of $\mathcal{C}^{\mathcal{T}}$ is small as well. This is desirable for convolutional codes because the complexity of the decoding algorithm increases with δ.

Theorem 9. *Let $\mathcal{T}$ be an $(n-1,w)$-DTS and consider the matrix $\begin{bmatrix} A_0^\top & \cdots & A_\mu^\top \end{bmatrix}^\top$ defined as in the previous construction. Denote by w_j the minimal column weight of $\begin{bmatrix} A_0^\top & \cdots & A_j^\top \end{bmatrix}^\top$. For $I \subset \{1,\dots,\mu+1\}$ and $J \subset \{1,\dots,n(\mu+1)\}$ we define $[\mathcal{H}^{\mathcal{T}}]_{I;J}$ as the submatrix of $\mathcal{H}^{\mathcal{T}}$ with row indices I and column indices J. Assume that for all I, J with $|I| = |J| \le w$ and $j_1 := \min(J) \le n-1$ and I containing the indices where column j_1 is nonzero, we have that the first column of $[\mathcal{H}^{\mathcal{T}}]_{I;J}$ is not contained in the span of the other columns of $[\mathcal{H}^{\mathcal{T}}]_{I;J}$. Then*

(i) $\mathrm{d}_{\mathrm{free}}(\mathcal{C}^{\mathcal{T}}) = w+1$,
(ii) $d_j^c = w_j + 1$.

Proof: (i) Without loss of generality, we can assume that the first entry of H_0 is nonzero. Let $M \subset \{1,\dots,\delta+1\}$ with $|M| = w$ be the set of positions where the first column of $\mathcal{H}$ (and hence also the first column of the sliding parity-check matrix) has nonzero entries. Denote the values of these nonzero entries by $d_1,\dots,d_w$. Then, $v(z) = \sum_{i=0}^{r} v_i z^i$ with $v_0 = [1\ 0\cdots 0\ -d_1]$ and $v_i = \begin{cases} [0\cdots 0] & \text{for } i+1 \notin M \\ [0\cdots 0\ -d_{i+1}] & \text{for } i+1 \in M \end{cases}$ for $i \ge 1$ is a codeword with $\mathrm{wt}(v(z)) = w+1$. Hence $\mathrm{d}_{\mathrm{free}} \le w+1$.

Assume by contradiction that there exists a codeword $v \neq 0$ with weight $d \le w$. We can assume that $v_0 \neq 0$, i.e. there exists $i \in \{1,\dots,n\}$ with $v_{0,i} \neq 0$. One knows $\mathcal{H}^{\mathcal{T}} v^\top = 0$. Of this homogeneous system of equations, where we consider the nonzero components of $v_0, v_1, \dots, v_{\deg(v)}$ as variables, we take only the rows where column i of $\mathcal{H}^{\mathcal{T}}$ has nonzero entries. We end up with a homogeneous system with w equations and d variables, whose coefficient matrix has full column rank according to the assumptions of the theorem. This implies $v = 0$, what is a contradiction.
(ii) The result follows from Theorem 2 with an analogue reasoning as in part (i). ∎

Remark 10. With the assumptions of Theorem 9, one has $d_j^c = \mathrm{d}_{\mathrm{free}}(\mathcal{C}^{\mathcal{T}})$ for $j \ge \mu$. Moreover, one achieves higher column distances (especially for small j) if the elements of $\mathcal{T}$ are small.

Proposition 11. *If N is the maximal message length, i.e. for any message v, $\deg(v)+1 \le N/n$, then the sliding parity-check matrix of a convolutional code derived in Definition 4 has density*

$$\frac{w(n-1)+1}{\mu n + N}.$$

Proof: To compute the density of a matrix, one has to divide the number of nonzero entries by the total number of entries. The result follows immediately. ∎

Theorem 12. *Let $\mathcal{T}$ be an $(n-1,w)$-DTS with scope $m(\mathcal{T})$ and $\mathbb{F}_q$ be the finite field with q elements with $q > (n-1)\delta + 1 = (n-1)(m(\mathcal{T})-1)+1$. Let $\mathcal{C}^{\mathcal{T}}$ be the rate $(n-1)/n$ convolutional code defined over $\mathbb{F}_q$ from $\mathcal{T}$, with $\mathcal{H}^{\mathcal{T}}$ as defined in* (3)*. Then, all the 2×2 minors in $\mathcal{H}^{\mathcal{T}}$ that are non-trivially zero are non-zero.*

Proof: The only 2×2 minors to check are the ones of the form $\begin{vmatrix} a_1 & a_2 \\ a_3 & a_4 \end{vmatrix}$. By definition of DTS, the support of any column of $\mathcal{H}^{\mathcal{T}}$ intersects the support of its shift at most once. This ensures that the columns of all these minors are the shift of two different columns of $\bar{H}^{\mathcal{T}}$. Moreover, all the elements

$$\mathcal{H}^{\mathcal{T}} = \begin{bmatrix}
\alpha & \alpha^2 & 1 & & & & & & & & & & & & & & & \\
\alpha^2 & \alpha^4 & 0 & \alpha & \alpha^2 & 1 & & & & & & & & & & & & \\
0 & 0 & 0 & \alpha^2 & \alpha^4 & 0 & \alpha & \alpha^2 & 1 & & & & & & & & & \\
0 & \alpha^8 & 0 & 0 & 0 & 0 & \alpha^2 & \alpha^4 & 0 & \alpha & \alpha^2 & 1 & & & & & & \\
0 & 0 & 0 & 0 & \alpha^8 & 0 & 0 & 0 & 0 & \alpha^2 & \alpha^4 & 0 & \alpha & \alpha^2 & 1 & & & \\
\alpha^6 & 0 & 0 & 0 & 0 & 0 & 0 & \alpha^8 & 0 & 0 & 0 & 0 & \alpha^2 & \alpha^4 & 0 & \alpha & \alpha^2 & 1
\end{bmatrix}$$

Fig. 1. Sliding parity-check matrix for the code in Example 5.

$$\mathcal{H}^{\mathcal{T}} = \begin{bmatrix}
\alpha & 0 & 1 & & & & & & & & & & & & & & & \\
\alpha^2 & \alpha^4 & 0 & \alpha & 0 & 1 & & & & & & & & & & & & \\
0 & \alpha^6 & 0 & \alpha^2 & \alpha^4 & 0 & \alpha & 0 & 1 & & & & & & & & & \\
0 & 0 & 0 & 0 & \alpha^6 & 0 & \alpha^2 & \alpha^4 & 0 & \alpha & 0 & 1 & & & & & & \\
0 & \alpha^{10} & 0 & 0 & 0 & 0 & 0 & \alpha^6 & 0 & \alpha^2 & \alpha^4 & 0 & \alpha & 0 & 1 & & & \\
\alpha^6 & 0 & 0 & 0 & \alpha^{10} & 0 & 0 & 0 & 0 & 0 & \alpha^6 & 0 & \alpha^2 & \alpha^4 & 0 & \alpha & 0 & 1
\end{bmatrix}$$

Fig. 2. Sliding parity-check matrix for the code in Example 6.

in the minor are powers of α. In particular, let $1 \leq i, r \leq \delta$, $0 \leq j, k \leq n-1$ (note that $j < k$ or $k < j$ according to which columns from $\bar{H}^{\mathcal{T}}$ are involved in the shifts). Hence we have that:

$$\begin{vmatrix} a_1 & a_2 \\ a_3 & a_4 \end{vmatrix} = \begin{vmatrix} \alpha^{ij} & \alpha^{lk} \\ \alpha^{(i+r)j} & \alpha^{(l+r)k} \end{vmatrix} = \alpha^{ij}\alpha^{(l+r)k} - \alpha^{lk}\alpha^{(i+r)j} = \alpha^{ij+lk}(\alpha^{rk} - \alpha^{rj})$$

which is 0 if and only if $rk = rj \mod (q-1)$. Since it holds that $0 \leq j < k \leq n-1$ or $0 \leq k < j \leq n-1$ and $1 \leq r \leq \delta$, this can not happen. ∎

Theorem 13. *Let $\mathcal{T}$ be an $(n-1, w)$-DTS with scope $m(\mathcal{T})$, $w \geq 3$ and $\mathbb{F}_q$ be the finite field with $q > 2$ elements with $q = p^N$, where $N > (\delta-1)(n-2) = (m(\mathcal{T})-2)(n-2)$. Let $\mathcal{C}^{\mathcal{T}}$ be the rate $(n-1)/n$ convolutional code defined over $\mathbb{F}_q$ from $\mathcal{T}$, with $\mathcal{H}^{\mathcal{T}}$ as defined in* (3)*. Then, all the 3×3 minors in $\mathcal{H}^{\mathcal{T}}$ that are non-trivially zero are non-zero.*

Proof: We need to distinguish different cases.

Case I. The 3×3 minors are of the form $\begin{vmatrix} a_1 & a_2 & a_3 \\ a_4 & a_5 & a_6 \\ a_7 & a_8 & a_9 \end{vmatrix}$, with $a_i \neq 0$ for any i. As we observed in Theorem 12, in this case all the columns are shifts of three different columns from $\bar{H}^{\mathcal{T}}$. Hence we have that, given $1 \leq i, l, t \leq \delta - 3$, $r, s > 0$, with $r \neq s$ and $2 \leq i + r, l + r, t + r \leq \delta - 1$ and $4 \leq i + r + s, l + r + s, t + r + s \leq \delta$, the minors are given by

$$\begin{vmatrix} a_1 & a_2 & a_3 \\ a_4 & a_5 & a_6 \\ a_7 & a_8 & a_9 \end{vmatrix} = \begin{vmatrix} \alpha^{ij} & \alpha^{lk} & \alpha^{tm} \\ \alpha^{(i+r)j} & \alpha^{(l+r)k} & \alpha^{(t+r)m} \\ \alpha^{(i+r+s)j} & \alpha^{(l+r+s)k} & \alpha^{(t+r+s)m} \end{vmatrix}.$$

This determinant is 0 if and only if

$$\alpha^{rk+rm+sm} + \alpha^{rm+rj+sj} + \alpha^{rj+rk+sk} = \quad (5)$$
$$\alpha^{rk+rj+sj} + \alpha^{rj+rm+sm} + \alpha^{rk+rm+sk}. \quad (6)$$

Without loss of generality we can assume that $j < k < m$ and it turns out that the maximum exponent in equation (5) is $rk + rm + sm$ while the minimum is $rk + rj + sj$. Let $M := rk + rm + sm - (rk + rj + sj)$. We immediately see that the maximum value for M is $(\delta - 1)(n - 2)$ hence this determinant can not be zero because α is a primitive element for $\mathbb{F}_q$ and, by assumption, $q = p^N$, where $N > M$.

Case II. The 3×3 minors are of the form $\begin{vmatrix} a_1 & a_2 & 0 \\ 0 & a_3 & a_4 \\ a_6 & 0 & a_5 \end{vmatrix}$. Arguing as before, we notice that given $1 \leq i, l, t \leq \delta - 3$, $r, s > 0$, with $r \neq s$ and $2 \leq i + r, l + r, t + r \leq \delta - 1$ and $4 \leq i + r + s, l + r + s, t + r + s \leq \delta$, the minors are given by

$$\begin{vmatrix} \alpha^{ij} & \alpha^{lk} & 0 \\ 0 & \alpha^{(l+r)k} & \alpha^{(t+r)m} \\ \alpha^{(i+r+s)j} & 0 & \alpha^{(t+r+s)m} \end{vmatrix} = \alpha^{ij+lk+tm+rm}(\alpha^{rk+sm} + \alpha^{rj+sj}).$$

This determinant is 0 whenever $r(k-j) + s(m-j) - (q-1)/2 = 0 \mod (q-1)$. If $q > 2(n-3) + 2(\delta-2)(n-2) + 1$ this never happens. And this is the case for our field size assumption.

Case III. The 3×3 minors are of the form $\begin{vmatrix} a_1 & a_2 & 0 \\ a_3 & a_4 & a_5 \\ a_6 & 0 & a_7 \end{vmatrix}$. As in the first cases, we can assume that, for $1 \leq i, l, t \leq \delta - 3$, $r, s > 0$, with $r \neq s$ and $2 \leq i + r, l + r, t + r \leq \delta - 1$ and $4 \leq i + r + s, l + r + s, t + r + s \leq \delta$, the minor is given by

$$\begin{vmatrix} \alpha^{ij} & \alpha^{lk} & 0 \\ \alpha^{(i+r)j} & \alpha^{(l+r)k} & \alpha^{(t+r)m} \\ \alpha^{(i+r+s)j} & 0 & \alpha^{(t+r+s)m} \end{vmatrix}.$$

By following the reasoning of the previous cases, if $N > (\delta-1)(n-2)-1$, this determinant is nonzero which is always the case, because of the field size assumption. ∎

Example 14. In Example 5, one has $d_0^c = 2$, $d_1^c = d_2^c = d_3^c = d_4^c = 3$ and $d_5 = \mathrm{d_{free}} = 4$.

Example 15. In Example 6, one has $d_0^c = 1$, $d_1^c = 2$, $d_2^c = d_3^c = d_4^c = 3$ and $d_5 = \mathrm{d_{free}} = 4$.

Remark 16. With Theorems 12 and 13 we can ensure that the 4 and 6-cycles in the Tanner graph associated to codes $\mathcal{C}^{\mathcal{T}}$ defined over $q = p^N$, with $N > (\delta - 1)(n - 2)$ satisfy the FRC. This improves the performances of our NB-LDPC convolutional codes.

Moreover, it is possible to reduce the required field size for the construction of $\mathcal{C}^{\mathcal{T}}$ by restricting the conditions on the DTS $\mathcal{T}$ and still ensuring that all the 4 and 6-cycles satisfy the FRC. In particular, we can get rid of the *Case I* of Theorem 13 by imposing that the sets in $\mathcal{T}$ pairwise intersect at most twice and also the support of one column intersects the support of the shifts of any column at most twice, to ensure that all columns of $\mathcal{H}^{\mathcal{T}}$ intersect at most twice. We will leave these considerations for future works.

V. Conclusion and Future Research Works

In this paper, we gave a construction of rate $(n-1)/n$ convolutional codes over non-binary fields, generalizing a construction from Robinson and Bernstein, using difference triangle sets. We related the important parameters of the codes with the parameters of the considered DTS, pointing out how combinatorics can help in solving applied problems (in this case minimizing the degree δ of the code).

Generalizations of this work will be addressed in an extended version. In particular, minors of $\mathcal{H}^{\mathcal{T}}$ of larger size than 3×3 could be considered to derive convolutional codes with larger distances. Unfortunately, this may require a larger field size.

Moreover, Theorem 9, Remark 10 and Theorem 11 can be generalized to arbitrary rates k/n. However, it is not completely trivial anymore to compute the degree δ with the help of the parity-check matrix of the code.

REFERENCES

[1] B. Amiri, J. Kliewer, and L. Dolecek. Analysis and enumeration of absorbing sets for non-binary graph-based codes. *IEEE Transactions on Communications*, 62(2):398–409, 2014.

[2] M. Battaglioni, M. Baldi, F. Chiaraluce, and M. Lentmaier. Girth properties of time-varying SC-LDPC convolutional codes. In *2019 IEEE International Symposium on Information Theory (ISIT)*, pages 2599–2603. IEEE, 2019.

[3] Y. M. Chee and C. J. Colbourn. Constructions for difference triangle sets. *IEEE Transactions on Information Theory*, 43(4):1346–1349, 1997.

[4] Z. Chen, P. Fan, and F. Jin. Disjoint difference sets, difference triangle sets, and related codes. *IEEE Transactions on Information Theory*, 38(2):518–522, 1992.

[5] C. J. Colbourn. Difference triangle sets. *Chapter in The CRC Handbook of Combinatorial Designs by CJ Colbourn and J. Dintz*, pages 312–317, 1996.

[6] M. C. Davey and D. J. MacKay. Low density parity check codes over GF (q). In *1998 Information Theory Workshop (Cat. No. 98EX131)*, pages 70–71. IEEE, 1998.

[7] M. C. Davey and D. J. MacKay. Monte Carlo simulations of infinite low density parity check codes over GF(q). In *Proc. of Int. Workshop on Optimal Codes and related Topics*, pages 9–15. Citeseer, 1998.

[8] R. Gallager. Low-density parity-check codes. *IRE Transactions on Information Theory*, 8(1):21–28, 1962.

[9] H. Gluesing-Luerssen, J. Rosenthal, and R. Smarandache. Strongly-MDS convolutional codes. *IEEE Transactions on Information Theory*, 52(2):584–598, 2006.

[10] T. Klove. Bounds and construction for difference triangle sets. *IEEE Transactions on Information Theory*, 35(4):879–886, 1989.

[11] D. J. MacKay and R. M. Neal. Near shannon limit performance of low density parity check codes. *Electronics letters*, 32(18):1645–1646, 1996.

[12] J. L. Massey. Threshold decoding. 1963.

[13] C. Poulliat, M. Fossorier, and D. Declercq. Design of regular $(2, d_c)$-LDPC codes over GF(q) using their binary images. *IEEE Transactions on Communications*, 56(10):1626–1635, 2008.

[14] A. E. Pusane, R. Smarandache, P. O. Vontobel, and D. J. Costello. Deriving good LDPC convolutional codes from LDPC block codes. *IEEE Transactions on Information Theory*, 57(2):835–857, 2011.

[15] J. P. Robinson and A. Bernstein. A class of binary recurrent codes with limited error propagation. *IEEE Transactions on Information Theory*, 13(1):106–113, 1967.

[16] S.-Y. Tong. Systematic construction of self-orthogonal diffuse codes. *IEEE Transactions on Information Theory*, 16(5):594–604, 1970.

[17] A. Wyner and R. Ash. Analysis of recurrent codes. *IEEE Transactions on Information Theory*, 9(3):143–156, 1963.

[18] H. Zhou and N. Goertz. Cycle analysis of time-invariant LDPC convolutional codes. In *2010 17th International Conference on Telecommunications*, pages 23–28. IEEE, 2010.